I. Understanding Identity Theft and How to Assist its Victims

Each year millions of Americans discover that a criminal has fraudulently used their personal information to obtain goods and services and that they have become victims of identity theft. Under federal law, identity theft occurs when someone uses or attempts to use the sensitive personal information of another person to commit fraud.[1] A wide range of sensitive personal information can be used to commit identity theft, including a person's name, address, date of birth, Social Security number (SSN), driver's license number, credit card and bank account numbers, phone numbers, and even biometric data like fingerprints and iris scans.

The most common form of identity theft, and the main focus of this guide, involves the fraudulent use of a victim's personal information for financial gain. There are two main types of such financial frauds: 1) the use of the victim's existing credit, bank, or other accounts; or 2) the opening of new accounts in the victim's name. Many times victims experience both.

The opening of a new account causes greater harm to the victim than the misuse of an existing account. A victim of existing account misuse often can resolve problems directly with the financial institution, which will consider the victim's prior relationship with the institution and the victim's typical spending and payment patterns. On the other hand, a victim of new account identity theft usually has no preexisting relationship with the creditor to help prove she is not responsible for the debts. The new account is usually reported to one or more credit reporting agency (CRA), where it then appears on the victim's credit report. Since the thief does not pay the bills, the account goes to collections and appears as a bad debt on the victim's credit report. Often, the victim does not discover the existence of the account until it is in collections. So, the victim must prove to the creditor that she is not responsible for the account and clear the bad debt information from her credit report. Other types of identity theft besides account fraud are listed in the Glossary at **Appendix A.1.**

This guide will provide you with step-by-step information to assist identity theft victims from the initial screening call to the final letter. Specifically, it will help you assist a victim in achieving the following three goals: (1) stopping or minimizing further fraud from occurring; (2) proving that identity theft has occurred and that the victim is not responsible for debts incurred in her name; and (3) correcting any errors on the victim's credit report to restore her financial reputation and credit score.

The guide initially assumes a worst-case scenario, where the victim has experienced new account identity theft, and a fraudulent new account has been added to her credit report. The

[1] The Fair Credit Reporting Act (FCRA) defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." "Identifying information" is "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person . . . " Fair Credit Reporting Act, Pub.L. 108-159, sec 111, 15 U.S.C. § 1681a; 16 C.F.R §603.2.

guide presents simpler alternatives for victims who have not experienced new account identity theft and who typically do not need to clear their credit report.

This guide also assumes that many victims of identity theft are able to resolve their concerns by themselves, once they have been informed of the steps they need to take. Your office will want to encourage most victims to take as many steps as possible on their own, and offer to stay in touch to monitor success and provide additional assistance as needed. In some instances, however, it may be clear from the initial screening call that the victim will be unable to undo the harms caused by the theft of her identity. Victims may need your immediate direct assistance when:

- their age, health, language proficiency, or economic situation create barriers for them in disputing and correcting errors in their records;
- they are sued by creditors attempting to collect debts incurred by an impostor;
- they are being harassed by creditors attempting to collect debts incurred by an impostor,
- creditors or CRAs are being uncooperative; or
- their case is complex or involves non-financial identity theft.

A. Preparing to Assist an Identity Theft Victim

Victims who have experienced the more serious forms of identity theft often report emotional harm, including feeling an enormous sense of vulnerability and a diminished trust in others. The Office of Victims of Crime has created a tutorial on interviewing identity theft victims with tips on how to attune your approach to their emotional needs. You and those in your office who will be interacting with identity theft victims may want to go through the tutorial. It can be found at www.ovcttac.gov/IdentityTheft.

B. The Initial Screening Call

When a victim contacts your office, you will need to gather the facts to determine if identity theft has occurred, whether the victim needs your immediate direct assistance, and what assistance, if any, your office may provide. To make these determinations, you should ask the following questions:

- What facts lead the caller to believe that her personal information has been misused?
- How and where did the identity thief misuse the information?
- When and how did the caller discover the misuse or fraud?
- What harm has the caller suffered as a result of the identity theft?

If you confirm that the caller is an identity theft victim, you should advise her to take the following three steps immediately to prevent further harm, whether the identity theft involves

new or existing accounts.[2] These three steps are: 1) placing an initial fraud alert on her credit reports; 2) obtaining and reviewing her credit reports for evidence of additional identity theft; and 3) cancelling any compromised bank, credit card, or other accounts. You also may wish to provide the caller with additional resources, as described below, as well as advise her of the importance of documenting her efforts.

1. *Initial Fraud Alert*

Placing an initial fraud alert on credit reports will reduce the risk that an identity thief will open new accounts in the victim's name. An initial fraud alert stays on the victim's credit file for 90 days, and can be renewed every 90 days. Identity theft victims can place an initial 90-day fraud alert by contacting one of the following three CRAs. That CRA must, in turn, contact the other two CRAs on the victim's behalf:

> **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
>
> **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
>
> **Equifax**: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
>
> **Note:** A CRA may request additional proof of identity to place the initial fraud alert, and it may ask the victim to answer challenge questions – information in her credit report that only the victim would be expected to know. (For more information on proof of identity, see **Appendix A.3**.)

If your client experienced new account identity theft, she should consider placing a credit freeze on her credit report. For a more extensive discussion of credit freezes, see **Section II.A** of this guide.

2. *Copies of Credit Reports*

Once your client has placed an initial fraud alert on her credit report, she is entitled to a free credit report from each of the three CRAs. These free copies of credit reports are in addition to the right all consumers have to receive a free copy of their credit report annually. For more information on free annual reports, see **Appendix D.3.**

---

[2] The screener should use his judgment as to whether to advise the victim to take additional steps. For example, the risk of additional harm to a victim who has experienced only the loss of an existing credit card is relatively low. That victim can usually resolve all issues by contacting the credit card issuer.

After placing a fraud alert on her credit report, your client should receive a confirmation letter from each CRA advising her how to order a free credit report. Some CRAs may allow the victim to place the fraud alert online. If so, she may be able to order and view her credit report online immediately upon placing the fraud alert. If the victim does not receive a CRA's confirmation letter, she should contact the CRA directly.

> **Note**: When a victim places a fraud alert on her credit report, the CRA may offer to sell her products or services, such as credit monitoring or identity theft insurance. For more information on these products, see "To Buy or Not to Buy" at **Appendix D.9.** Later, when the victim calls the CRA to order the free credit report she is entitled to in conjunction with the fraud alert, the CRA may first direct the victim's attention to ordering her free annual credit report, before explaining how she can order the one associated with the fraud alert. This can confuse the victim and lead her to order the free annual report rather than the credit report that is hers by right after placing a fraud alert.

Victims should review their credit report for any accounts they did not open, debts they did not incur, and credit inquiries from companies they have not contacted. They should promptly contact any companies where their credit report indicates this has occurred and follow step 3, below. Guidance on "How to Read a Credit Report" is at **Appendix D.4.**

3. *Contact Creditors and Other Organizations*

Where accounts were fraudulently opened or misused, victims should immediately telephone the creditor's fraud department, not the consumer services department, to explain that they are victims of identity theft and direct the creditor to close the account and remove the charges.

Where a new account was opened, the victim will need to prove that she did not create the debt. One method to prove new account identity theft is the FTC's Identity Theft Affidavit, which is addressed in greater detail below and in **Section II.B.A**. However, some companies require victims to submit the company's own proprietary forms. The victim should ask each company she contacts whether it accepts the FTC Identity Theft Affidavit.

Where only unauthorized charges to an existing account were involved, the victim should call the company for instructions. The detailed information in an FTC Identity Theft Affidavit or its equivalent should not be needed where only an existing account was misused.

Some creditors designate a specific mailing address to which the victim must send correspondence concerning the dispute of a debt, or to request documents related to the identity theft. Victims should ask about these designated addresses in their initial phone call.

4. *Additional Resources*

Based upon your conversation with the caller, you may discover that the victim has already taken the above three steps to address the theft. At this stage, you should determine whether the victim is willing to take additional self-help steps on her own with occasional phone support from your office, or seems likely to require hands-on assistance from your office in moving forward with the self-help process. The checklist in **Appendix B.2** can help you figure out where your client is in the recovery process and what she needs to do next. You may wish to send her educational materials (**Appendix D**) and sample letters (**Appendix C**) that she can use to address her situation.

Much of this guidance is also available from the FTC, either at www.ftc.gov/idtheft, or through the toll free hotline at 1-877- ID-THEFT. The FTC provides assistance in English and Spanish. There are other valuable online resources for victims listed in **Appendix A.5.**

In most cases, you may wish to schedule a follow-up call about two weeks later to see how your client's initial self-help efforts are going. You should advise the client to contact your office at any time if she has any questions or if her first self-help efforts are not fully successful.

5. *Maintaining a Log*

Whether the victim experienced new account fraud or existing account misuse, and whether she wishes to act alone or with your assistance, you should instruct her, from the outset, to keep a complete record of all calls and letters she generates or receives, and the amount of time she spends and expenses she incurs, in the course of her recovery. Documentation is critical for establishing the facts and providing a basis for damages should the matter go to litigation or criminal prosecution. Under a new law, victims may be able to recover the value of the time they spent recovering from the identity theft if the case is prosecuted in Federal court and the judge orders the defendant to pay restitution.[3]. (For a copy of this statute, see **Appendix E.2**.) The sample "Chart Your Course of Action" at **Appendix D.10** is a useful model for record-keeping. A more comprehensive and extensive sample record-keeping log, provided with the consent of the Victims Initiative for Counseling, Advocacy, and Restoration of the Southwest (VICARS), is at **Appendix D.11.**

C. Preparing for a First Meeting

About two weeks after the screening call, you may wish to contact the victim to see how her efforts are paying off. Victims of existing account misuse that do not have exacerbating issues such as language deficiencies, pending lawsuits, or complex cases would rarely need to meet with you personally. For these victims, you can normally provide additional guidance during the follow-up phone call that will enable them to continue their successful self-help actions.

---

[3] Identity Theft Enforcement and Restitution Act of 2008, 18 U.S.C. § 3663.

Victims of new account fraud – in addition to taking the three immediate steps discussed above – usually will have to take several additional steps to address their problems. Specifically, they will need to begin the process of writing letters and creating written documentation to continue resolving their problems. In some cases, victims will be able to do this on their own with only phone support from you. If it appears that a victim may need help in executing some of the additional self-help steps, you may wish to arrange a first meeting, particularly if you wish to assist the victim in preparing documents.

To prepare for the meeting, you should advise the victim to gather supporting documents, including the following:

- Government-issued IDs;
- Utility bills or other monthly statements showing the victim's address;
- One or more credit reports showing fraudulent activity;
- Collection letters, credit card or bank statements, or any cards or merchandise received but not ordered; and
- A log showing any action that the victim may have taken to date.

D. The Intake Meeting

The objective of the intake meeting is to determine the type and amount of assistance the victim may need and to develop an action plan. The Checklist at **Appendix B.2** can help you hone in on what steps the victim has taken, what problems may have arisen, and what steps need to be taken next.

1. *Get to Know Your Client*

Understanding your client's identity theft experience is key to providing appropriate assistance. In addition to direct financial losses, some victims may have:

- suffered secondary harm, such as damage to their credit standing or to their reputation;
- expended significant time attempting to correct credit reports and obtain new identity documents;
- suffered revictimization, or chronic identity theft, whereby their stolen identity is used repeatedly by different thieves; and
- suffered severely debilitating emotional and physical effects, including depression, anxiety, and sometimes becoming suicidal.

2. *Review the Facts*

The intake meeting provides an opportunity to review in more detail the facts gathered during the initial call. Specifically, you should determine what type of identity theft has occurred. **Appendix B.1** contains a chart that provides sample interview questions that can help you get a better understanding of your client's situation. It also indicates the sections of the guide that relate to the type of identity theft your victim has experienced and the concerns she may be facing. You should also make a list of additional documents that the client may need to provide, if the client did not bring all requested documents to the meeting or it appears from the first meeting that additional documents are needed.

E. Make an Action Plan

Having determined the nature of your client's ongoing problems, you should explain to your client the tools and possible legal solutions available to address the identity theft. Your Action Plan should cover the following steps, as appropriate.

1. *Documenting the Crime*

If your client has experienced new account identity theft, the next phase in her recovery will be to document the crime. Such documentation will be necessary to prove to a creditor that she is not responsible for the fraudulent new account or to exercise certain legal rights, such as clearing fraudulent accounts from her credit report and prohibiting creditors from selling the fraudulent debts. Specifically, your client may need an Identity Theft Affidavit or an Identity Theft Report (a detailed police report). Below are steps your client can take, alone or with your assistance, to prepare for obtaining these documents.

a. *File a Complaint with the FTC*

The first step in documenting identity theft is to file a complaint with the FTC. Your client can file a complaint online by going through the guided interview process at www.ftccomplaintassistant.gov. Before filing her complaint, the victim should gather as much information as possible about the details of the crime. This would include a credit report from at least one of the three major CRAs, any collection letters or bills he received for accounts she did not open or charges she did not authorize, and any credit cards or other items she received, but had not ordered.

The complaint asks for the following information:

- The victim's full name, any other or previously used names;
- Current and/or recent address and the address at the time the crime occurred, if different from the current address;
- Social Security Number;

- Date of Birth;
- What the victim knows about who committed the crime or how her information was stolen;
- What the victim knows about the fraudulent transactions, including institution names, types of account or transactions involved, account numbers, dates the accounts were opened or misused, and dollar amounts related to the fraudulent activity; and
- Whether the victim has been able to obtain a police report, and if so, the details.

> **Note**: It is important to note that victims are not required to file a written complaint with the FTC in order to pursue their legal rights to remedy identity theft. Victims may also file a complaint, but without the ability to receive a printed copy, by calling the FTC's Identity Theft Hotline, toll-free: 1-877-ID-Theft (438-4338); TTY: 1-866-653-4261; or writing the Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. The FTC does not investigate or prosecute individual identity theft cases. The FTC enters the complaints into its Consumer Sentinel Network and makes them available to enforcement agencies throughout the country for their investigations. The complaints also help the FTC identify general trends in identity theft and violations of the FCRA. Victims who do not want to provide their personal information can file their complaints with the FTC anonymously.

b. *Prepare an FTC Identity Theft Affidavit*

Next, your client should prepare an Identity Theft Affidavit, which many creditors accept to dispute fraudulent new accounts. It also will assist your client in preparing an Identity Theft Report, as explained below.

By completing the FTC complaint online, your client will be then able to print a copy of her Affidavit, with most of the information filled in automatically. Specifically, after she has completed the online complaint's guided interview process and has hit the "Submit" button, a page will appear that will provide a link to print the Affidavit. Alternatively, victims can print out a blank copy of the Identity Theft Affidavit from the FTC Identity Theft website at www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf . The Affidavit contains a block for notarization, or alternatively, a witness signature. A copy of the Affidavit is available at **Appendix D.6.** For more information about the FTC Identity Theft Affidavit, see **Section II.B.A.**

You may wish to fill in the Identity Theft Affidavit form by hand as you get to know your client and review the facts with her. Filling out a hard copy of the Affidavit as you interview your client serves dual purposes: you will gain a comprehensive understanding of your client's experience and identify knowledge gaps that need to be addressed, and you will provide her with a document to reference as she goes through the FTC's online complaint filing process, which collects much of the same information.

c. *File a Police Report*

The next step in documenting identity theft is to obtain an Identity Theft Report, which will enable the victim to take advantage of certain rights provided under the FCRA. An Identity Theft Report is a police report that contains information specific enough for a CRA or creditor to determine the legitimacy of the identity theft claims. This is usually more detailed than a typical police report. For more information about Identity Theft Reports, see **Section II.B.B.** Identity theft victims will also need a police report in order to obtain a company's business records related to its transactions with the identity thief.

If possible, your client should file her report with the local police in person. Your client should bring a copy of her FTC ID Theft Affidavit, as well as documentation supporting her proof of identity and evidence of the crime. The goal is to get a copy of a detailed police report that incorporates as much detail as possible about the facts of the crime. Your client can request that the police attach or incorporate her Identity Theft Affidavit to the department's basic police report form. There are signature blocks on the Affidavit for the victim and the officer.

Further, an officer whose department participates in the FTC's fraud database, the Consumer Sentinel Network, can update the victim's FTC complaint from his own computer. The officer can add the official police report number assigned by the department, as well as the department's name and phone number. The officer can also print out a revised version of the victim's Identity Theft Affidavit with this information included. If the department does not participate in Consumer Sentinel, the officer can write the police report number and department information on the victim's copy of the Identity Theft Affidavit and sign it, thus turning the Affidavit into an Identity Theft Report.

Police sometimes are reluctant to provide victims with a police report. Although some states require police to write reports for identity theft crimes, in other jurisdictions the officials may feel that they have higher priority matters to handle, or may not understand the importance of the police report in victim recovery. If your client has difficulty obtaining a police report, **Section II.B.C** describes a number of steps that she can take.

Once your client obtains an Identity Theft Report, she will then be able to prevent most further harm and to restore her financial reputation.

2. *Using the Documents to Effectuate Self-Help Recovery*

a. *Send Creditors and Other Organizations Written Dispute Letters*

Victims should follow up their initial telephone calls to creditors with written dispute letters, including copies of their Identity Theft Affidavit, as described above. Some creditors may require the use of their own dispute forms, or require victims to have their Affidavits notarized. Your client should have asked about the Identity Theft Affidavit and any notarization requirement in her initial phone call. A police report should not be required as part of this written dispute, but some creditors may ask for one.

Victims may also want to include in their dispute letters a request for business records, such as any applications and records of transactions between the identity thief and the creditor. The creditor can require a police report before it provides the requested transaction records. More information about obtaining business records from companies can be found in **Section III.E**.

As mentioned above, some creditors designate a specific mailing address to which the victim must send correspondence concerning the dispute of a debt, or to request documents related to the identity theft. Your client should have asked about these designated addresses in her initial phone call. If there are no designated addresses, your client should write to the company at the address given for billing inquiries, not the address for sending payments. She should send her letters by certified mail, return receipt requested, in order to document what the company received and when. Sample dispute and document request letters can be found in **Appendix C**.

Once a victim resolves her identity theft dispute with a company, she should obtain a letter from the creditor or other institution stating that the disputed account is closed and the fraudulent debt discharged. This letter will be useful if errors relating to the account reappear on the victim's credit report, or if she is contacted again regarding the fraudulent debt.

b. *Fix Credit Reports*

Victims need to clear their credit reports of any accounts they did not open, debts they did not incur, and credit inquiries from companies they have not contacted. They should also correct any inaccuracies in their personal information -- such as their Social Security number, address, name or initials, and employers.

There are two ways to dispute incorrect information on a credit report. Victims can have inaccurate identity theft-related information permanently blocked from appearing on their credit report by using the streamlined procedures set forth in section 605B and 623(a)(6)(B) of the FCRA. Some examples of information victims might want to have permanently blocked could include fraudulent new accounts they did not open, credit inquiries initiated by an identity thief, and additional addresses or other information that does not relate to them. Victims must obtain an Identity Theft Report that is verified by the police to use the procedures of section 605B and 623(a)(6)(B). For more detailed information on the procedures for requesting a block of the identity theft-related information from a credit report, see **Section III.A**.

The other remedy available to victims to correct the erroneous information in their credit reports is using the dispute process available to all consumers under sections 611 and 623 of the FCRA. A correction might be preferred to a complete and permanent block when the account affected by identity theft is one that, when restored to its pre-crime status, would significantly benefit the victim's credit score. Another situation might be when the victim has closed the existing account that was damaged by the identity thief, and opened another account with the same company. In such a case, the favorable account history associated with the damaged account might be transferred to the new account. The procedures for disputing information on a credit report can be found at **Section III.B.**

c. *Monitor Credit Reports*

After fixing the errors in their credit reports, victims should monitor their reports for new fraudulent activity for the first year after the identity theft is discovered. Victims also can take advantage of the free annual report, and should consider staggering their requests among the three CRAs to receive one every four months so as to obtain more continuous coverage over the 12-month period. Victims with an extended fraud alert may use their second free credit report to continue their monitoring during the 12-month period after the alert was placed.

d. *Consider an Extended Fraud Alert*

Your client should consider placing an extended, seven-year fraud alert on her credit report. This will make it more difficult for an identity thief to open new accounts in the victim's name because potential creditors have to contact the victim by phone, in person, or by another means indicated by the victim before extending new credit, raising credit limits, or issuing additional cards.

The requirements for placing an extended, seven-year fraud alert differ slightly for each company. One requirement common to all companies is that the victim must provide an Identity Theft Report with her request for the extended fraud alert. Because not all police departments provide police reports to identity theft victims, the FTC's Rule on Related Identity Theft Definitions, 16 C.F.R. Part 603.3, specifies that a print-out of a Complaint filed with the FTC will suffice for obtaining an extended fraud alert. Company-specific information on how to obtain a seven-year fraud alert can be found on their websites, at the links indicated below:

> **Experian*:*** Mail - PO Box 9554, Allen, TX 75013; website with information, including link to form: https://www.experian.com/consumer/cac/InvalidateSession.do?code=SECURITYALERT
>
> **TransUnion:** Mail - PO Box 6790, Fullerton, CA 92834; website with information (no form): http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/fraudAlert.page
>
> **Equifax:** Mail - Information Services, LLC, PO Box 105069, Atlanta, GA 30348-5069; website with information, including link to form: http://www.equifax.com/answers/set-fraud-alerts/en_cp

For more information on fraud alerts, see **Section II.A** of this guide. For advice on placing fraud alerts with specialty CRAs, such as those dealing with offers of insurance or landlord/tenant issues, see **Section IV.G**.

F. Attorney Intervention

If your client can't take all of the recovery steps mentioned above independently, or continues to have problems after taking those steps, you may need to intervene on her behalf and directly contact the companies and entities involved. These entities may ask that you provide a Power of Attorney or other client authorization before discussing the victim's financial affairs. **Appendix A.4** provides a standard authorization form that should satisfy these purposes.

1. *Contact the Creditor or CRA*

Depending on the nature and status of your client's issues, you may decide to communicate with your client's creditors or the relevant CRAs with a phone call, a letter inviting a phone call, or a letter requesting a written response. Some straightforward identity theft problems can be resolved with a single phone call from you to the attorney or a senior supervisor at the company involved. Generally, it is preferable to communicate in writing so as to document your efforts. In some situations, however, immediate action is necessary, such as

when a mortgage closing is being delayed due to the identity theft; in these cases, it may be preferable to contact the relevant parties by phone and follow up in writing, if warranted.

2. *Sample Letters*

Should you conclude that it is necessary to write to your client's creditors, this guide provides a number of sample attorney letters. You should know, however, that the sample attorney letters address only a small number of the potential problems that victims encounter. Further, the applicability of the different remedies available to identity theft victims under the statutes can be very fact-specific. Accordingly, you should adapt your letter to the particular circumstances of your client's complaint and be as specific as possible. At a minimum, you should insert a statement of the facts and an explanation of the remedies the victim is due. If the company's response has been inadequate, you should explain why the company is not meeting its legal obligations.

3. *Closing Letter*

Finally, you may want to provide your client with a closing letter summarizing the problems you worked on as her representative, the entities that you contacted, and the results you obtained. This will serve as a reference for both of you if your client is re-victimized and gets in touch with your office.

G. Private Rights of Action and Consumer Protection Remedies

This guide focuses on resolving victims' issues in a non-litigation context. The federal consumer credit protection statutes,[4] however, provide private rights of action under some circumstances. Accordingly, you should review each applicable statute carefully to determine the scope and type of remedies that may be available to your client. These can provide remedies for violations, including compensatory damages, attorneys' fees, statutory damages, punitive damages, and/or injunctive and declaratory relief. **Section III** provides notes on the availability of federal private rights of action for the provisions it covers.

Many of the statutes provide for administrative enforcement at the federal and/or state level, either in lieu of or in addition to private enforcement. If you believe a creditor or CRA has violated the federal statutes discussed in this guide, please report this information to the Federal Trade Commission at https://www.ftccomplaintassistant.gov/ or via email to probonoguide@ftc.gov.

Complaints filed with the FTC are available through the FTC's Consumer Sentinel Network to federal, state, and local law enforcement including the banking agencies that regulate financial institutions.

---

[4] *See, e.g.*, Fair Credit Billing Act, 15 U.S.C. § 1601; Fair Credit Reporting Act, 15 U.S.C. § 1681; and Fair Debt Collection Practices Act, 15 U.S.C. § 1692.